

Dialog DataStar[options](#)[logout](#)[feedback](#)[help](#)[databases](#)[easy search](#)**Advanced Search:****Inspec - 1898 to date (INZZ)**[limit](#)

Search history:

No.	Database	Search term	Info added since	Results	
CP		[Clipboard]		0	-
1	INZZ	bit ADJ adj2 ADJ slic\$3 AND (cryptograph\$3 OR DES OR AES)	unrestricted	0	-
2	INZZ	bit ADJ slic\$3 AND (cryptograph\$3 OR DES OR AES)	unrestricted	111	show titles
3	INZZ	limit set 2 YEAR < 2001	unrestricted	109	show titles
4	INZZ	3 AND (sbox OR substitution ADJ box)	unrestricted	0	-

[hide](#) | [delete all search steps...](#) | [delete individual search steps...](#)Enter your search term(s): [Search tips](#) ☐ Thesaurus mapping Information added since: or:
(YYYYMMDD)[search](#)☐ Images

Select special search terms from the following list(s):

- ☒ Publication year 1950-
- ☒ Publication year 1898-1949
- ☒ Inspec thesaurus - browse headings
- ☒ Inspec thesaurus - enter a term
- ☒ Classification codes A: Physics, 0-1
- ☒ Classification codes A: Physics, 2-3
- ☒ Classification codes A: Physics, 4-5
- ☒ Classification codes A: Physics, 6


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

bit slice cryptography engine

1776

- 2000

Search

Ad
Sc
Sc
Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 69 for **bit slice cryptography engine**. (
All Results[J Goodman](#)[M Rosner](#)[A Dancy](#)[A Chandrakasan](#)[C MIT](#)

[An energy/security scalable encryption processor using an embedded variable voltage DC/DC converter - all 10 versions »](#)

J Goodman, AP Dancy, AP Chandrakasan, C MIT - Solid-State Circuits, IEEE Journal of, 1998 - [ieeexplore.ieee.org](#)

... The encryption **engine** utilizes an algorithm known as the ... multipliers for RSA-based encryption schemes are ... functions and memory locally within the **bit slice**. ...

Cited by 45 - [Related Articles](#) - [Web Search](#)

[IDEA: A Cipher for Multimedia Architectures? - all 8 versions »](#)

H Lipmaa - Selected Areas in **Cryptography**: 5th Annual International ..., 1999 - [books.google.com](#)

... In particular, **bit-slice** MMX implementations of different block ciphers should be ... additionally using 32-bit and 64-bit operations (eg ... [au/mkwan/bitslice/Uelcome](#). ...

Cited by 26 - [Related Articles](#) - [Web Search](#)

[RNS-modulo reduction upon a restricted base value set and its applicability to RSA cryptography - all 2 versions »](#)

J Schwemmlin, KC Posch, R Posch - Computers & Security, 1998 - Elsevier

... technologies (0,35-0,18pm), such an encryption **engine** might fit ... paper, where a modified

RSA encryption scheme (MRSA) is ... set out of six, one in **bit slice** 0.2 ...

Cited by 8 - [Related Articles](#) - [Web Search](#)

[A 12 Gbps DES Encryptor/Decryptor Core in an FPGA - all 4 versions »](#)

S Trimberger, R Pang, A Singh - Cryptographic Hardware and Embedded Systems--CHES 2000: ..., 2000 - [books.google.com](#)

... four hours, yielding a circuit that encrypts or decrypts a 64-bit block every ...

[au/bitslice/nonstd](#) ... 7. Schneier, B., Applied **Cryptography**, John Wiley and Sons, 1996 ...

Cited by 26 - [Related Articles](#) - [Web Search](#)

[\[PDF\] Energy Scalable Reconfigurable Cryptographic Hardware for Portable Applications - all 3 versions »](#)

JR Goodman - 2000 - [www-mtl.mit.edu](#)

... 172 5.7.4 Reconfigurable Datapath **Bitslice**. ... amount of computation required to factor

n-bit moduli. ... 4-6 Top-level architecture of the encryption **engine** (QRG). ...

Cited by 19 - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)

[A bit-serial implementation of the international data encryption algorithm](#)

[IDEA - all 5 versions »](#)

MP Leong, OYH Cheung, KH Tsoi, PHW Leong - Field-Programmable Custom Computing Machines, 2000 IEEE ..., 2000 - [ieeexplore.ieee.org](#)

Page 1. A Bit-Serial Implementation of the International Data Encryption Algorithm IDEA MP Leong, OYH Cheung, KH Tsoi and PHW Leong ...

Cited by 29 - [Related Articles](#) - [Web Search](#)


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

serpent aes

1776

- 2000

Search

Ad
Sc
Sc
Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 19,100 for **serpent aes**. (0.23 seconds)
All Results[E Biham](#)[R Anderson](#)[L Knudsen](#)[S Chari](#)[D Rumelhart](#)

[PDF] [Serpent: A Proposal for the Advanced Encryption Standard - all 40 versions »](#)

R Anderson, E Biham, L Knudsen - NIST **AES** Proposal, Jun, 1998 - ftp.cl.cam.ac.uk

... 16-round **Serpent** would be as secure as triple-DES, and twice as fast as DES. However, **AES** may persist for 25 years as a standard and a further 25 years in ...

Cited by 119 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[PDF] [Hardware Evaluation of the AES Finalists - all 10 versions »](#)

T Ichikawa, T Kasuya, M Matsui - Proc. 3th **AES** Candidate Conference, New York, April, 2000 - csrc.nist.gov

... We therefore decided to analyze the **AES** finalists using ... results show that Rijndael is the fastest as expected and ... is even faster than DES, and **Serpent** is the ...

Cited by 61 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[An FPGA implementation and performance evaluation of the Serpent block cipher - all 12 versions »](#)

AJ Elbirt, C Paar - Proceedings of the 2000 ACM/SIGDA eighth international ..., 2000 - portal.acm.org

... Mbit/s [6]. For this study, the **AES** candidate chosen was the Serpent encryption algorithm. As will be shown in Section 5, the **Serpent** algorithm was chosen ...

Cited by 35 - [Related Articles](#) - [Web Search](#)

[PS] [Serpent: A Flexible Block Cipher With Maximum Assurance - all 10 versions »](#)

R Anderson, E Biham, L Knudsen - The First **AES** Candidate Conference, 1998 - sunsite.rediris.es

... bitslice techniques for DES encryption (as opposed to ... **Serpent** was therefore designed so that all operations ... of implementations, see our **AES** submission package ...

Cited by 18 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[PDF] [Comparison of the hardware performance of the AES candidates using reconfigurable hardware - all 12 versions »](#)

K Gaj, P Chodowicz - Proc. 3rd Advanced Encryption Standard (**AES**) Candidate ..., 2000 - csrc.nist.gov

... It is over twice as slow than the next slowest candidate (RC6), and over 8 times slower than the fastest **AES** cipher (**Serpent**). It ...

Cited by 79 - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent - all 26 versions »](#)

J Kelsey, T Kohno, B Schneier - Proceedings of the Seventh Fast Software Encryption Workshop, 2000 - Springer

... decryptions. 1 Introduction MARS [BCD+98] and **Serpent** [ABK98] are block ciphers that have been proposed as **AES** candidates [NIST97a,NIST97b]. ...

Cited by 29 - [Related Articles](#) - [Web Search](#)

[PDF] [Performance analysis of AES candidates on the 6805 CPU core - all 19](#)